UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,062	07/30/2001	Keith Alexander Harrison	30006786-2	2570

7590 06/23/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KEITH ALEXANDER HARRISON and RICHARD BROWN

Appeal 2009-005936
Application 09/918,062
Technology Center 2400

Decided: June 23, 2010

Before ALLEN R. MACDONALD, *Vice Chief Administrative Patent Judge*, JAMES D. THOMAS and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 (2002) from a final rejection of claims 1-19. We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We AFFIRM.

A. INVENTION

According to Appellants, the invention relates to a fax transmission protocol which can be used in conjunction with the existing standard fax protocols to provide additional security in fax transmission and/or delivery (Spec. 1, ll. 3-6).

B. ILLUSTRATIVE CLAIM

Claim 1 is exemplary and is reproduced below:

1. A method of delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the method comprising:

receiving and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender;

obtaining a second token of the sender relating to the first token of the sender;

obtaining a first token of the intended recipient;

decoding the encrypted digest using the second token of the sender;

using a hash algorithm to create a digest of the document;

comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;

decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station;

comparing the decrypted identification data with contents of the independently verifiable data record to determine the authenticity of the recipient of the document; and

releasing the document when the intended recipient has proved their identity by use of the first token of the intended recipient that is uniquely related to the second token of the intended recipient.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Clark	5,448,045	Sep. 5, 1995
Linsker	5,598,473	Jan. 28, 1997
Davis	5,633,932	May 27, 1997
Mazzagatte	6,862,583 B1	Mar. 1, 2005

Menezes, Handbook of Applied Cryptography 397-405 (CRC Press, 1996).

Claims 1-12 and 14-19 stand rejected under 35 U.S.C. § 103(a) over the teachings of Linsker in view of Mazzagatte, Davis and Menezes.

Claim 13 stands rejected under 35 U.S.C. § 103(a) over the teachings of Linsker in view of Mazzagatte, Davis and Menezes, and further in view of Clark.

II. ISSUE

Did the Examiner err in finding that the combination of Linsker in view of Mazzagatte, Davis and Menezes would have taught or suggested "decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station" (claim 1), as Appellants contend? In particular, the issue turns on whether combining Davis's teachings of encryption of data at a sending node with Menezes' teachings of encryption using the recipient's identifier would have suggested encryption data "encrypted using a second token of the recipient by a transmitting station" as required by claim 1.

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Davis

1. Davis discloses a system including a sending node that has access to a public key of the printing node and uses this public key to encrypt a header and document before transmission to the printing node over the communication link (Abstract).

Menezes

2. Menezes discloses authentication for communication between A and B, wherein B sends a random number r_B to A, A encrypts identification data with encryption algorithm E_K using the random number r_B received from B, and B decrypts the received message and checks that the random number matches that sent to A (p. 401, 10.16.2).

IV. ANALYSIS

Claims 1-12 and 14-19

Appellants contend that "*Mazzagatte* teaches that encryption and decryption operations are both performed at a print node" (App. Br. 13), "*Linsker* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted" (App. Br. 13-14), "*Menezes* does not teach or suggest using a token of an intended recipient" (App. Br. 14), and Davis's "header information is not encrypted using a public key of an intended recipient" (*Id.*).

The Examiner explains that "Mazzagatte was relied upon for more general teachings of verifying the intended recipient of a document" (Ans. 12), "Linsker was relied upon for teachings of the claimed features related to the verification of an unknown sender of a document and/or of that document itself" (Ans. 13), "Menezes clearly does disclose using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient" (*id.*), and that, as Appellants admit, "Davis discloses encrypting identifying information using a public key of a printing node" (Ans. 14). The Examiner further explains that though "Linsker, Mazzagatte, and Davis 'do not explicitly disclose that the challenge/response protocol decrypts encrypted identification data with the recipient's private key' …, Menezes was relied upon for a teaching of such a limitation" (*id.*). Thus, the Examiner concludes that "in response to Appellant's arguments against the references individually" (Ans. 11), "at least in combination, Menezes and Davis at the very least suggest encrypting identifying information with the public key of the intended recipient and transmitting that information from the sender" (Ans. 14).

By contending that Linsker, Mazzagatte, Davis and Menezes do not disclose the claimed invention (App. Br. 13-14), Appellants appear to be arguing that *individually*, these references do not disclose the features of claim 1. However, as the Examiner notes (Ans.12), the Examiner rejects claim 1 over the *combined* teachings of Linsker, Mazzagatte, Davis and Menezes, and what the combined teachings *would have suggested* to one of ordinary skill in the art. One cannot show nonobviousness by attacking

references individually where the rejections are based on combinations of references. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

Davis discloses a sending node that uses a public key to encrypt a header and document before transmission to the printing node over the communication link (FF 1). An artisan skilled in the art would have understood Davis's sending node to be a transmitting station, and thus, would have understood Davis's encryption using a public key as encryption using a token by a transmitting station.

Menezes discloses encrypting identification data at station *A* using the random number received from station *B*, wherein, upon decryption, *B* checks whether the random number matches the random number that *B* sent (FF 2). The skilled artisan would also have understood Menezes to teach decoding encrypted identification data with a token of the intended recipient, wherein the identification data is encrypted using a token of the recipient.

We agree with the Examiner's conclusion that "at least in combination, Menezes and Davis at the very least suggest encrypting identifying information with the public key of the intended recipient and transmitting that information from the sender" (Ans. 14). Since Davis discloses encrypting data using a token by a transmitting station, we conclude that the combination of one known element (Menezes's encryption of identification data using a token of the recipient) with another (Davis's encryption by a transmitting station) would have yielded predictable results to one of ordinary skill in the art at the time of the invention. That is, we

find that combining the use a token of the recipient to encrypt as taught by Menezes to Davis's encryption by a transmitting station is no more than a simple arrangement of old elements, with each performing the same function it had been known to perform, yielding no more than one would expect from such an arrangement. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

The skilled artisan would "be able to fit the teachings of multiple patents together like pieces of a puzzle" since the skilled artisan is "[a] person of ordinary creativity, not an automaton." *Id.* at 420-21. Appellants have presented no evidence that combining Menezes's teaching of using the token of the recipient to encrypt to the encryption of Davis was "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418-19).

As for independent claims 9, 18 and 19, Appellants merely repeat the arguments that the references do not individually teach all the limitations of the claimed invention (App. Br. 16-26). However, as discussed above regarding claim 1, the Examiner rejects the claims over the *combined* teachings of Linsker, Mazzagatte, Davis and Menezes, and we agree with the Examiner that the combined teachings *would have suggested* the claimed invention to one of ordinary skill in the art.

Accordingly, we conclude that the Examiner did not err in rejecting independent claim 1 and independent claims 9, 18, and 19 falling therewith,

and claims 2-8, 10-12, and 14-17 respectively depending therefrom under 35 U.S.C. § 103(a).

Claim 13

Appellants do not provide separate arguments with respect to the rejection of claim 13 depending from claim 11. Therefore, we find that the Examiner also did not err in rejecting dependent claim 13 under 35 U.S.C. § 103(a) over Linsker in view of Mazzagatte, Davis, Menezes, and further in view of Clark.

V. CONCLUSIONS

(1) The Examiner did not err in concluding that claims 1-12 and 14-19 are unpatentable under 35 U.S.C. § 103(a) over the teachings of Linsker in view of Mazzagatte, Davis and Menezes.

(2) The Examiner did not err in concluding that claim 13 is unpatentable under 35 U.S.C. § 103(a) over the teachings of Linsker in view of Mazzagatte, Davis, Menezes, and Clark.

(3) Claims 1-19 are not patentable.

VI. DECISION

We affirm the Examiner's rejections of claims 1-19 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

peb

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION
P.O. BOX 272400
FORT COLLINS, CO 80527-2400